ORIGINAL

AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* "Apple iPhone, model number MG642LL/A, serial number DNPND0H7G, Seized on April 20, 2017 from Aiman Alexander Ataba, currently in the Custody of of FBI in Orange, California"	)	Case No. 8:17-MJ-00123

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4/20/2017 at 3:02 pm

Judge's signature

City and state: Santa Ana, California

Hon. Douglas F. McCormick, U.S. Magistrate Judge
Printed name and title

GWS:sia

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant ~~and inventory~~ left with:
8:17-MJ-00123	4-20-17; Approx 3:15 pm	both provided to AZAbal's Atty on 4-24-17

Inventory made in the presence of :
FBI personnel only

Inventory of the property taken and name of any person(s) seized:
[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

* See 1 PAGE Attachment hereto.

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 4-27-2017

Executing officer's signature

BRAD HOWARD - FBI Special Agent

Printed name and title

AFFIDAVIT

I, Brad Howard, being duly sworn, do hereby depose and state:

I. INTRODUCTION

1. I am a Special Agent ("SA") for the Federal Bureau of Investigation ("FBI") in Santa Ana, California and have been so employed for 20 years. I was trained at the FBI Academy in Quantico, Virginia. For the last 14 years I have primarily worked on investigations of white collar crime, including high yield investment programs, Ponzi Schemes and other mail and wire fraud schemes. I have attended training on white collar and financial crimes, including money laundering, with the FBI in Quantico and other locations. Prior to my employment with the FBI, I was an attorney for nine years. Also, I graduated from college with a business degree with an emphasis in accounting.

2. In the course of my investigations, I have participated in surveillance, participated in search warrants both in my cases and cases handled by other agents, and interviewed a number of targets and defendants in fraud cases.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are

related in substance and in part only and are not intended to be direct quotes.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a search warrant for evidence of violations of 18 U.S.C. §§ 1341 (mail fraud) and 1957 (money laundering)(collectively, the "Subject Offenses") on an Apple iPhone, model number MG642LL/A, serial number DNPND0H7G..., seized from Aiman Alexander ATABA at the time of his arrest on April 20, 2017 (the "SUBJECT DEVICE").

5. The SUBJECT DEVICE is more specifically described in Attachment A to the search warrant applications. The items to be seized from the SUBJECT DEVICE are set forth in Attachment B to the search warrant application. Attachments A and B are incorporated herein by reference.

III. STATEMENT OF PROBABLE CAUSE

6. On April 19, 2017, ATABA was indicted by a grand jury in Orange County, California, on eight counts of mail fraud in violation of 18 U.S.C. § 1341 and three counts of money laundering in violation of 18 U.S.C. § 1957. A copy of the indictment is attached as Exhibit 1 and incorporated by reference. Also on April 19, 2017, a search warrant was authorized by the Hon. Douglas F. McCormick, United States Magistrate Judge, for the office used by ATABA in Fountain Valley. A copy of the search warrant application and affidavit is attached as Exhibit 2 and incorporated by reference.

7. As set forth in the indictment and search warrant affidavit, there is probable cause to believe that ATABA has committed mail fraud and money laundering in connection with his solicitation of investments in a company called Innovation Validation & Design Technologies, LLC ("IVDT"). As described in the indictment and affidavit, ATABA solicited more than $640,000 from a victim with promises that the money would be used to develop a stem cell device, and that the victim would receive warrants entitling him to purchase stock in IVDT at a discount. As set forth in the indictment and affidavit, ATABA used the money instead for personal expenses. The victim received neither any money back nor any stock in IVDT.

8. On April 20, 2017, ATABA was arrested on the charges in the attached indictment. He had the SUBJECT DEVICE in his possession when he was arrested.

9. On April 6, 2017, I spoke with the victim in this case who said that about a week earlier ATABA called him, but the victim did not answer.

10. As set forth in the attached affidavit, there is probable cause to believe that ATABA has retained evidence concerning IVDT. In addition, given that ATABA tried to contact the victim within the last month, there is probable cause to believe the SUBJECT DEVICE may contain evidence relating to IVDT.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

11. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical

manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive

could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular

user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of

peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time. An off-site review is appropriate based on the anticipated volume of electronic data that will likely be collected. Investigators will arrange for a team of will be searching through financial records, escrow documents, The DEA

will provide a team assigned to the Document and Media Exploitation (DOMEX) program. DOMEX provides tactical assistance in the collection, triage and analysis of large volumes of physical and digital evidence. DOMEX will attempt to scan these documents on site in order to avoid disrupting any legitimate business. Investigators will collect all closed escrow documents for evaluation, which will be scanned off-site. Investigators will make arrangements to provide any specific "closed escrow" document files within seven calendar days upon request.

12. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

13. For all the reasons described above, there is probable cause to believe that evidence of violations of the Subject Offenses, as described above and in Attachment B of this affidavit, will be found in the search of SUBJECT DEVICE.

/s/
BRAD HOWARD, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me on
April 20, 2017
DOUGLAS F. McCORMICK

HON. DOUGLAS F. MCCORMICK
UNITED STATES MAGISTRATE JUDGE

Non-Instrumentality Protocol

ATTACHMENT A

Premises to be searched

The premises to be searched is further described as an Apple iPhone, model number MG642LL/A, serial number DNPND0H7G... seized from Aiman Alexander ATABA on April 20,2017, currently in the custody of the FBI in Orange, California.

ATTACHMENT B

Items to be Seized

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence of violations of 18 U.S.C. § 1341 and 18 U.S.C. § 1957 from January 1, 2012, to the present, namely:

a. All records, documents, programs, applications, or materials related to Innovation Validation & Design Technologies, LLC ("IVDT").

b. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Non-Instrumentality Protocol

d. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

2. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

a. Prior to reading any document or other piece of evidence ("document") in its entirety, law enforcement personnel

conducting the investigation and search and other individuals assisting law enforcement personnel in the search (the "Search Team") will conduct a limited review of the document in order to determine whether or not the document appears to contain or refer to communications between an attorney, including John Kremer, or to contain the work product of an attorney, and any person ("potentially privileged information"). If a Search Team member determines that a document appears to contain potentially privileged information, the Search Team member will not continue to review the document and will immediately notify a member of the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case). The Search Team will not further review any document that appears to contain potentially privileged information until after the Privilege Review Team has completed its review.

b. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to the Search Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then

the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

c. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Search Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Non-Instrumentality Protocol

Digital Evidence

3. The Search Team will search for digital devices capable of being used to facilitate the subject offenses or capable of containing data falling within the scope of the items to be seized. The Privilege Review Team will then review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

4. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

5. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without first obtaining an extension of time order from the Court.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like "John Kremer" or email addresses, and generic words such as "privileged" or "work product." The Privilege Review Team will conduct an initial

review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

7. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team.

Non-Instrumentality Protocol

Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

9. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

Non-Instrumentality Protocol

10. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

12. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

13. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the

time for searching the device has expired) absent further court order.

14. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

15. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

16. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

Non-Instrumentality Protocol

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

17. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Non-Instrumentality Protocol

EXHIBIT 1

Under Seal

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

September 2016 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. AIMAN ALEXANDER ATABA, aka AIMAN WAJIH ALATABEH, Defendant.	No. SA CR 17-00024 I N D I C T M E N T [18 U.S.C. § 1341: Mail Fraud; 18 U.S.C. § 1957: Money Laundering; 18 U.S.C. § 2(b): Causing an Act to Be Done]

The Grand Jury charges:

COUNTS ONE THROUGH EIGHT

[18 U.S.C. §§ 1341, 2(b)]

A. INTRODUCTORY ALLEGATIONS

At all times relevant to this Indictment:

1. Defendant AIMAN ALEXANDER ATABA also known as AIMAN WAJIH ALATABEH ("ATABA"), solicited investments in Innovation Validation & Design Technologies, LLC ("IVDT").

////

////

B. THE SCHEME TO DEFRAUD

2. Beginning in or around January 2012, and continuing to at least August 2016, in Orange County, within the Central District of California, and elsewhere, defendant ATABA and others known and unknown to the Grand Jury, knowingly and with the intent to defraud, devised, participated in, and executed a scheme to defraud investors as to material matters and to obtain money from investors, by means of materially false and fraudulent pretenses, representations, and promises, and the concealment of material facts.

3. The fraudulent scheme was designed to operate, and did operate, as follows:

a. Through false and fraudulent statements and written materials, defendant ATABA and others attempted to induce and did induce at least one victim to invest in IVDT.

b. To obtain the victim's money, defendant ATABA and others made material omissions and false promises and statements, including, without limitation, that IVDT was building a device for stem cell research that would be used in hospitals.

4. To execute the aforementioned scheme, defendant ATABA, together with others known and unknown to the Grand Jury, knowingly engaged in fraudulent and deceptive acts, practices and devices, and caused false and deceptive statements to be communicated to, and material information to be concealed and omitted from, victims, including, without limitation, the following:

a. That IVDT was building a device for stem cell research that would be used in hospitals;

b. That money invested by victims would be used to develop and sell the stem cell device;

c. That stock warrants sent to victims after they invested would enable them to purchase IVDT stock at a discount; and

d. IVDT was on the verge of being acquired, which would result in a big payout to investors.

5. At the time defendant ATABA made and caused these statements to be made to victims, such statements were false, and defendant ATABA knew they were false, in that:

a. Money invested by victims was not used to develop and sell a stem cell device to hospitals;

b. Victims were never able to exercise the stock warrants to acquire stock in IVDT;

c. IVDT was never on the verge of being acquired by another company; and

d. The money receive by IVDT from victims was diverted by defendant ATABA from the bank account of IVDT for his personal use, including approximately $350,000 in cash withdrawals, gambling, personal medical expenses, airline tickets, rental car fees, clothing, utilities, home goods, electronics, a vehicle, and restaurants.

6. By devising, executing, and participating in the above scheme, defendant ATABA induced at least one victim to invest more than $640,000 with IVDT.

////

C. USE OF THE MAILS

7. On or about the following dates, in Orange County, within the Central District of California, and elsewhere, for the purpose of executing and attempting to execute the above-described scheme to defraud, defendant ATABA willfully caused the following items to be sent and delivered by a private or commercial interstate carrier according to the directions thereon:

COUNT	DATE	ITEM MAILED
ONE	5/29/12	Check no. 17791 in the amount of $32,850 from victim W.D. to IVDT
TWO	10/1/12	Check no. 18645 in the amount of $45,000 from victim W.D. to IVDT
THREE	2/1/13	Check no. 19565 in the amount of $45,220 from victim W.D. to IVDT
FOUR	8/27/13	Check no. 20855 in the amount of $100,000 from victim W.D. to IVDT
FIVE	2/20/14	Check no. 22073 in the amount of $150,000 from victim W.D. to IVDT
SIX	2/23/15	Check no. 24605 in the amount of $100,000 from victim W.D. to IVDT
SEVEN	6/16/15	Check no. 25392 in the amount of $150,000 from victim W.D. to IVDT
EIGHT	11/13/15	IVDT Warrant Certificate from IVDT to victim W.D.

COUNTS NINE THROUGH ELEVEN

[18 U.S.C. §§ 1957, 2(b)]

8. The Grand Jury repeats, realleges, and incorporates paragraphs 1 through 7 of this Indictment as though fully set forth herein in their entirety.

9. On or about the dates set forth below, in Orange County, within the Central District of California, and elsewhere, defendant ATABA, knowing that the funds involved represented the proceeds of some form of unlawful activity, engaged, and willfully caused others to engage in, the following monetary transactions affecting interstate commerce, in criminally derived property of a value greater than $10,000, which property, in fact, was derived from specified unlawful activity, that is, mail fraud, in violation of Title 18, United States Code, Section 1341:

COUNT	DATE	TRANSACTION
NINE	8/29/13	Deposit of check no. 1036 in the amount of $36,400 from the account of IVDT at Bank of America into the account of IVDT at Chase Bank
TEN	12/21/13	Purchase of Toyota Rav 4 from Auto Nation with check no. 1033 in the amount $25,355.56 from the account of IVDT at Chase Bank

COUNT	DATE	TRANSACTION
ELEVEN	2/25/14	Deposit of check no. 1037 in the amount of $55,000 from the account of IVDT at Bank of America into the account of IVDT at Chase Bank

A TRUE BILL

_____

Foreperson

SANDRA R. BROWN
Acting United States Attorney

Joe McNally FOR

LAWRENCE S. MIDDLETON
Assistant United States Attorney
Chief, Criminal Division

DENNISE D. WILLETT
Assistant United States Attorney
Chief, Santa Ana Branch Office

GREGORY W. STAPLES
Assistant United States Attorney

EXHIBIT 2

Magistrate Case Initiating Documents

8:17-mj-00121 USA v. SEARCH WARRANT

UNITED STATES DISTRICT COURT for the CENTRAL DISTRICT OF CALIFORNIA

Notice of Electronic Filing

The following transaction was entered by Staples, Gregory on 4/19/2017 at 10:36 AM PDT and filed on 4/19/2017

Case Name: USA v. SEARCH WARRANT
Case Number: 8:17-mj-00121
Filer: USA
Document Number: 1

Docket Text:
APPLICATION FOR A SEARCH AND SEIZURE WARRANT filed by Plaintiff USA. (Not for Public View pursuant to the E-Government Act of 2002) (Attachments: # (1) Proposed Warrant) (Attorney Gregory W Staples added to party USA(pty:pla)) (Staples, Gregory)

8:17-mj-00121-1 Notice has been electronically mailed to:

8:17-mj-00121-1 Notice has been delivered by First Class U. S. Mail or by other means BY THE FILER to :

The following document(s) are associated with this transaction:

Document description: Main Document
Original filename:N:\TempAUSA\Greg Staples\Search Warrants\4-19-17 \CAC.SA.MJ1700121.20170419.GS.Application for SW.pdf
Electronic document Stamp:
[STAMP cacdStamp_ID=1020290914 [Date=4/19/2017] [FileNumber=23375919-0] [72ae651ff40549b214a475225b306b3521c845648528c7daa550dbb9b70677aa66f 278dc80d72a80c7aa29ce219a1b5dd8daac1d016776072cacfc268e4ab7d4]]
Document description: Proposed Warrant
Original filename:N:\TempAUSA\Greg Staples\Search Warrants\4-19-17 \CAC.SA.MJ1700121.20170419.GS.SW.pdf
Electronic document Stamp:
[STAMP cacdStamp_ID=1020290914 [Date=4/19/2017] [FileNumber=23375919-1] [7c25900c10112883dfcce58b29ecd377b4404e8e2ff838150eaa6e6e3f3d9772d42 444fbd80bbb20a7704103d64e5bdab190706dd69da7364b33810ed91efb79]]

AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
17280 Newhope Street, Suite 8
Fountain Valley, California

Case No. 8:17-MJ-00121

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1957	Money Laundering

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Brad Howard - FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Santa Ana, California

Hon. Douglas F. McCormick, U.S. Magistrate Judge
Printed name and title

AUSA: Gregory W. Staples x3535

AFFIDAVIT

I, Brad Howard, being duly sworn, do hereby depose and state:

I. INTRODUCTION

1. I am a Special Agent ("SA") for the Federal Bureau of Investigation ("FBI") in Santa Ana, California and have been so employed for 20 years. I was trained at the FBI Academy in Quantico, Virginia. For the last 14 years I have primarily worked on investigations of white collar crime, including high yield investment programs, Ponzi Schemes and other mail and wire fraud schemes. I have attended training on white collar and financial crimes, including money laundering, with the FBI in Quantico and other locations. Prior to my employment with the FBI, I was an attorney for nine years. Also, I graduated from college with a business degree with an emphasis in accounting.

2. In the course of my investigations, I have participated in surveillance, participated in search warrants both in my cases and cases handled by other agents, and interviewed a number of targets and defendants in fraud cases.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are

related in substance and in part only and are not intended to be direct quotes.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a search warrant for evidence of violations of 18 U.S.C. §§ 1341 (mail fraud) and 1957 (money laundering) (collectively, the "Subject Offenses") at the office of Aiman Alexander ATABA located at 17280 Newhope Street, Suite 8, Fountain Valley, California (the "SUBJECT PREMISES").

5. The SUBJECT PREMISES are more specifically described in Attachment A to the search warrant applications. The items to be seized from the SUBJECT PREMISES are set forth in Attachment B to the search warrant application. Attachments A and B are incorporated herein by reference.

III. STATEMENT OF PROBABLE CAUSE

6. Beginning in approximately May 2016, I conducted a few interviews with victim W.D., who lives in San Bernardino County. W.D. told me that beginning in January 2012 he began receiving telephone calls from a person identifying himself as "Alex Julian" of Innovation Validation & Design Technologies, LLC ("IVDT"). Over the course of several calls, ATABA, who resides in Irvine, told W.D. that IVDT was developing a device to assist with stem cell research. ATABA told W.D. that when developed, the device would be sold to hospitals. ATABA told W.D. his money would be used to develop and sell the device. In return

for his investment, W.D. would receive stock warrants that would allow him to purchase IVDT stock at a discount.

7. Over the course of the next three years, W.D. made eight investments totaling more than $640,000 in IVDT, for which he received stock warrants signed by ATABA. I reviewed bank statements and copies of canceled checks, and saw the following investments in IVDT by W.D.:

1/28/12	Check no. 17085 in the amount of $25,000
5/29/12	Check no. 17791 in the amount of $32,850
10/1/12	Check no. 18645 in the amount of $45,000
2/1/13	Check no. 19565 in the amount of $45,220
8/27/13	Check no. 20855 in the amount of $100,000
2/20/14	Check no. 22073 in the amount of $150,000
2/23/15	Check no. 24605 in the amount of $100,000
6/16/15	Check no. 25392 in the amount of $150,000

The investment checks and warrants were sent via FedEx.

8. ATABA last spoke with W.D. in August 2016 when ATABA solicited W.D. for more money. I was with W.D. and recorded the call. During the call, ATABA pressured W.D. to invest more money claiming he could offer warrants to buy stock at 35 cents a share, but that it was for a limited time. After that, the price would be $1.60 a share. ATABA claimed that the "board" set the prices. When W.D. said he could not come up with more money right away, ATABA said he would talk to his manager and call back. When ATABA called back, he said that W.D. had a

payroll of $200,000 a month, and should have three to four months of payroll in reserve that could be used to invest. ATABA said IVDT had "booked a nice team of scientists" that were working on the product and the company was close to selling to "major customers" such as hospitals for "hundreds of millions of dollars." W.D. asked what had been done with the money he already invested. ATABA replied that it had been used to develop the "infrastructure" to get the company in the position it was in now. ATABA said the company was doing extremely well, and without W.D.'s investment it would not be ready now to do "big stuff." When W.D. asked if there were others like him, ATABA said they had more than 250 investors. ATABA said it was a great opportunity but would not last long. In the end, ATABA had W.D. agree to sign paperwork and forward a check that day, with the promise that the company would hold the check until the end of the week, when W.D. expected some money from a property sale. W.D. did not send a check.

9. I subpoenaed the records for all known bank accounts connected to ATABA and IVDT since January 2012. The records show the overwhelming source of deposits into the IVDT account was money from W.D. ATABA transferred money from the IVDT account to other accounts he controlled. ATABA made cash withdrawals in excess of $350,000, and used the balance of the money for gambling, home goods, electronics, airline tickets, rental cars, clothing and other personal expenses. ATABA also used money to buy a Toyota RAV 4, which was seized by the FBI in

December 2016.[1] There is no evidence that any of W.D.'s money was used to develop a stem cell device. There is no evidence of a board of directors, 250 investors, or a team of scientists involved with defendant. EDD records show no taxes paid by ATABA.

10. ATABA has an office in Fountain Valley. I interviewed the owner of the building on April 7, 2017. The owner told me ATABA has rented an office there for seven years. The last time the owner was in ATABA's office to repair something, there were only a few desks and computers, and not much else. The owner occasionally sees ATABA in the parking lot, but has never seen any other persons or employees enter ATABA's office. There is no sign on ATABA's office, and the owner had never heard of IVDT.

11. On April 6, 2017, I spoke with W.D. who told me that about a week earlier ATABA called him again, but W.D. did not answer.

12. On April 10, 2017, I conducted surveillance at the SUBJECT PREMISES. At about 9:15 a.m., I saw ATABA arrive and enter Suite 8. He was dressed casually and carried a black backpack.

---

[1] I know from speaking with FBI Special Agent Jessie Murray that ATABA is represented by John Kremer concerning the seizure of his Toyota. As set forth in Attachment B, a taint team will be used to screen and privileged communications that may be found among the seized items.

13. Based on my experience executing search warrants in fraud cases investigated by my and other FBI agents, I know that defendants engaged in fraud tend to keep records of their contacts with victims. For example, in *United States v. James Lewis*, SACR 04-16-CJC, I executed a search warrant at an office of a defendant engaged in a Ponzi scheme that spanned decades. I found records pertaining to victims dating back many years. In *United States v. Reed Diehl*, SACR 08-88-DOC, and in *United States v. Landreth*, SACR 06-106-CJC, I found the same types of records dating back many years. Based on these examples, as well as other searches I have participated in, I believe there is probable cause to believe that records pertaining to victim W.D. and IVDT with be found at the SUBJECT PREMISES.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

14. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding

analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory

or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack

space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for

by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was

not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time. An off-site review is appropriate based on the anticipated volume of electronic data that will likely be collected. Investigators will arrange for a team of will be searching through financial records, escrow documents, The DEA will provide a team assigned to the Document and Media Exploitation (DOMEX) program. DOMEX provides tactical assistance in the collection, triage and analysis of large volumes of physical and digital evidence. While searching at SUBJECT PREMISES 3 and 4, investigators anticipate identifying legitimate "open escrow documents." DOMEX will attempt to scan these documents on site in order to avoid disrupting any legitimate business. Investigators will collect all closed escrow documents for evaluation, which will be scanned off-site. Investigators will make arrangements to provide any specific "closed escrow" document files within seven calendar days upon request.

Non-Instrumentality Protocol

15. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

16. For all the reasons described above, there is probable cause to believe that evidence of violations of the SUBJECT OFFENSES, as described above and in Attachment B of this affidavit, will be found in the search of SUBJECT PREMISES.

BRAD HOWARD, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me on
April _____ , 2017

HON. DOUGLAS F. MCCORMICK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Premises to be searched

The premises to be searched is located at 17280 Newhope Street, Suite 8, Fountain Valley, California, 92708 and is further described as an office in a commercial office building located in the Los Caballeros Sports Village. The building is a two-story building with offices 7-13 on the ground floor and offices 14-20 upstairs. There is a smaller building with the same address with offices 1-6 next door to the left, as you look at the buildings. All office doors are visible from the parking lot. The building is a gold/tan color and has the number 17280 centered near the top of the building. Suite 8 is on the ground floor, next to suite 7. There is a stairway on the other side of Suite 7. Suite 8 has a brown French-type door with windows. The number 8 is directly above the door. There is a light fixture above the number 8. There are two white-framed windows to the right of the Suite 8 door. The door and the windows have blinds that are typically pulled down. There is a neatly trimmed Ficus tree in front of the two windows.

ATTACHMENT B

Items to be Seized

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence of violations of 18 U.S.C. § 1341 and 18 U.S.C. § 1957 from January 1, 2012, to the present, namely:

a. All records, documents, programs, applications, or materials related to Innovation Validation & Design Technologies, LLC ("IVDT").

b. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

Non-Instrumentality Protocol

d. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

2. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

a. Prior to reading any document or other piece of evidence ("document") in its entirety, law enforcement personnel

conducting the investigation and search and other individuals assisting law enforcement personnel in the search (the "Search Team") will conduct a limited review of the document in order to determine whether or not the document appears to contain or refer to communications between an attorney, including John Kremer, or to contain the work product of an attorney, and any person ("potentially privileged information"). If a Search Team member determines that a document appears to contain potentially privileged information, the Search Team member will not continue to review the document and will immediately notify a member of the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case). The Search Team will not further review any document that appears to contain potentially privileged information until after the Privilege Review Team has completed its review.

b. In consultation with a Privilege Review Team Assistant United States Attorney ("PRTAUSA"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to the Search Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then

the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

c. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRTAUSA. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Search Team. If appropriate based on review of particular documents, the PRTAUSA may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

Non-Instrumentality Protocol

Digital Evidence

3. The Search Team will search for digital devices capable of being used to facilitate the subject offenses or capable of containing data falling within the scope of the items to be seized. The Privilege Review Team will then review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

4. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

5. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without first obtaining an extension of time order from the Court.

6. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for on the digital devices, to include specific words like "John Kremer" or email addresses, and generic words such as "privileged" or "work product." The Privilege Review Team will conduct an initial

review of the data on the digital devices using the privilege key words, and by using search protocols specifically chosen to identify documents or data containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

7. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRTAUSA. Documents or data identified by the PRTAUSA after review as not potentially privileged may be given to the Search Team. If, after review, the PRTAUSA determines it to be appropriate, the PRTAUSA may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team.

Non-Instrumentality Protocol

Documents or data identified by the PRTAUSA after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

8. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

9. In performing the reviews, both the Privilege Review Team and the Search Team may:

a. search for and attempt to recover deleted, "hidden," or encrypted data;

b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and

c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

Non-Instrumentality Protocol

10. If either the Privilege Review Team or the Search Team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, they shall immediately discontinue the search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

11. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

12. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

13. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the

time for searching the device has expired) absent further court order.

14. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

15. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

16. In order to search for data capable of being read or interpreted by a digital device, the Search Team is authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

Non-Instrumentality Protocol

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

17. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Non-Instrumentality Protocol

Attachment 1

Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 318B-LA-6704960

On (date) 4-20-2017

item(s) listed below were:
- ☐ Received From
- ☐ Returned To
- ☐ Released To
- ☒ Seized

(Name) AIMAN ATABA

(Street Address) 17280 Newhope St. Suite 8

(City) Fountain Valley, CA 92708

Description of Item(s): Apple iPhone, model # MG642LL/A, Serial # DNPND0H7G - SEIZED from AIMAN ATABA @ time of arrest.

Received By: _____ (Signature)

Received From: AIMAN ATABA (Signature) (NO signature - has already left scene)